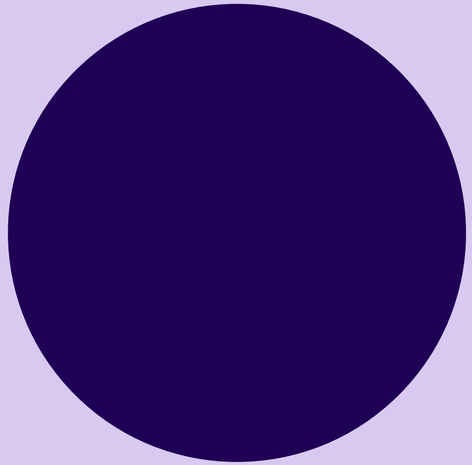
WithSecure™ Labs Whitepaper

WithSecure™ Security Cloud

Purpose, Function and Benefits



Contents

WithSecure™ Security Cloud in brief

The WithSecure™ Security Cloud (later: Security Cloud) is a cloud-based system for cyber threat analysis, designed, developed, and operated by WithSecure™ Corporation. At its core, the Security Cloud is a constantly-evolving repository of malware and other cyber threat-related data. Millions of endpoint clients, cloud-based systems, and internet-connected smart devices provide us with data to be analyzed. We then refine the data further, thanks to algorithms for threat intelligence, artificial intelligence, as well as the latest developments in machine learning. This deep analysis is carried out with the greatest respect to privacy and anonymity.

Every device that utilizes the Security Cloud benefits reciprocally from this data. The Security Cloud is comprised of multiple different components, each offering different benefits. These components are used in a multitude of different products, from endpoint clients to products protecting cloud-based systems. For example, threats that mobile devices encounter might produce data and give insights that contribute to protecting corporate networks of Fortune 500 companies, and vice versa. As the Security Cloud relies on data gathered from user devices to provide the service, WithSecure™ ensures that data protection and privacy policies are strictly upheld. Data collected from users is anonymized and no personally identifiable or other sensitive information is gathered. You can find more information about our data protection and privacy policies from the Security Cloud Privacy Policy.

The Security Cloud is a constantly-evolving system.
For this reason, the information in this document, including features and metrics, is subject to change. We update this document whenever major changes are made to the system. You can find the latest version of this document on the WithSecure™ website.

The benefits of the Security Cloud

Threat data from swarm attacks form a real-time protective network globally

New online threats are emerging all the time, and any user or company may encounter a new threat at any time. With a Security Cloud-enabled product, threat data goes directly to the Security Cloud; this includes the results of local analysis, behavioral and other metadata, as well as samples of files and web addresses. This data is further improved when other users encounter the same or similar threats. This makes it possible to create more effective and generic detections that provide protection from previously unseen but similar threats. All users of Security Cloud-enabled products subsequently benefit from this data and receive protection faster and more accurately. The Security Cloud forms an extensive protective network that grows more intelligent over time, and as more and more data feeds into the network and gets analyzed.

A winning combination of cloud analysis, human intelligence, and offline malware engines

Traditional cyber security products rely mainly on malware analysis engines installed locally on the device. Our latest product offerings combine traditional approaches to local analysis coupled with real-time analysis in the Security Cloud. The Security Cloud utilizes advanced technology and data that is unavailable on products locally, due to the computing resources required to perform machine learning on big datasets and dynamic analysis. This technology provides up-to-date information about new threats before they have been incorporated into commonly used threat databases.

Since WithSecure™ partners with numerous Fortune 500 companies, our consultants have the unique advantage of gaining access to the very cutting edge of malware when it is used –unsuccessfully– against our customers. This data is also fed into the Security Cloud, further increasing its value to other companies and users.

Strong protection with a light footprint for mobile devices

We understand that users are very sensitive to any kind of negative effects protection has on their devices. This is why mobile protection needs to be battery-efficient without sacrificing the quality of protection. The Security Cloud can operate as the sole engine for lightweight products that only requires users to give their consent when uploading certain files for analysis. Only a fraction of the files from users are uploaded, as in most cases the safety of the file can be analyzed with existing data. This behavior is resource-saving and optimal for mobile devices.

Strong protection for IoT devices

IoT devices in the home network can be protected with security software embedded on the router, providing browsing protection, tracking protection, botnet protection, and smart home security – all provided by the Security Cloud. Smart home security blocks malicious or compromised connections to and from smart home or IoT devices based on the URL or host name reputation. Tracking protection prevents tracking sites from following surfing habits and collecting data about users.

Botnet protection blocks traffic from compromised devices to an attacker's Command and Control center, adding another layer of detailed information about an infection. In addition, IoT devices can be protected with more advanced features such as advanced smart home security. This type of advanced feature blocks traffic from smart home or IoT devices based on the behavior analysis carried out on network activity in case anomalies are detected.

Advanced analysis for collaboration protection

Products that provide cloud-based collaboration for corporate customers rely heavily on the Security Cloud to carry out multi-stage analysis of the content. The analysis is a layered process that is triggered by the suspiciousness of the content, such as an email or calendar invite in the Microsoft Office 365 environment. Suspicious or unknown files are subjected to a deeper analysis with our cloud sandboxing technology, designed to prevent zero-day malware attacks and other advanced threats. The cloud sandbox runs the file to analyze its behavior. By focusing analysis on malicious behavior rather than static identifiers, the cloud sandbox can identify and block even the most sophisticated zero-day malware and exploits.

Multiple independent analysis methods ensure reliable analysis and elimination of false positives

The Security Cloud includes a comprehensive archive of files and web addresses. This collection is updated by several independently sourced sample feeds. Malicious and suspicious files uploaded for analysis by users of Security Cloud-enabled products form a part of this collection. A limited collection of common clean files is also included in this collection. The Security Cloud makes its final assessment based on multiple independent data sources and methods for dynamic and static analysis. This method makes it robust and less vulnerable to false positives than an anti-malware solution from a single source. The Security Cloud also periodically reanalyzes frequently encountered samples by using the latest information available to ensure continued accuracy.

Tracking malware behavior globally allows timely and precise mitigation of the impacts of malware

Real-time, global threat maps help us conduct timely and precise malware mitigation. With every client that communicates with the Security Cloud, we gain a granular, real-time view of how malware is distributed across the world, down to individual neighborhoods and devices. We can act quickly and perform targeted counter measures with our partners, without compromising the privacy of our users and the operations of business customers.

The Security Cloud saves on resources

Less computing power required

Security Cloud-enabled products can offload tasks to the Security Cloud that require heavy analysis computationally. This saves resources, and thus battery life, which is crucial on mobile devices and in other restricted environments, such as integrated cloud services, where heavy analysis of local malware is not possible.

Less device storage needed

The Security Cloud allows users to protect themselves without analysis engines taking up space on their local devices. This type of solution is ideal for devices where storage space is scarce, such as mobile devices, appliances, and tablets.

Bandwidth saved

The Security Cloud saves significant amounts of bandwidth by reducing or eliminating the need to update definition databases on the local device. Products with local engines need to update their definition databases frequently to have the latest information available.

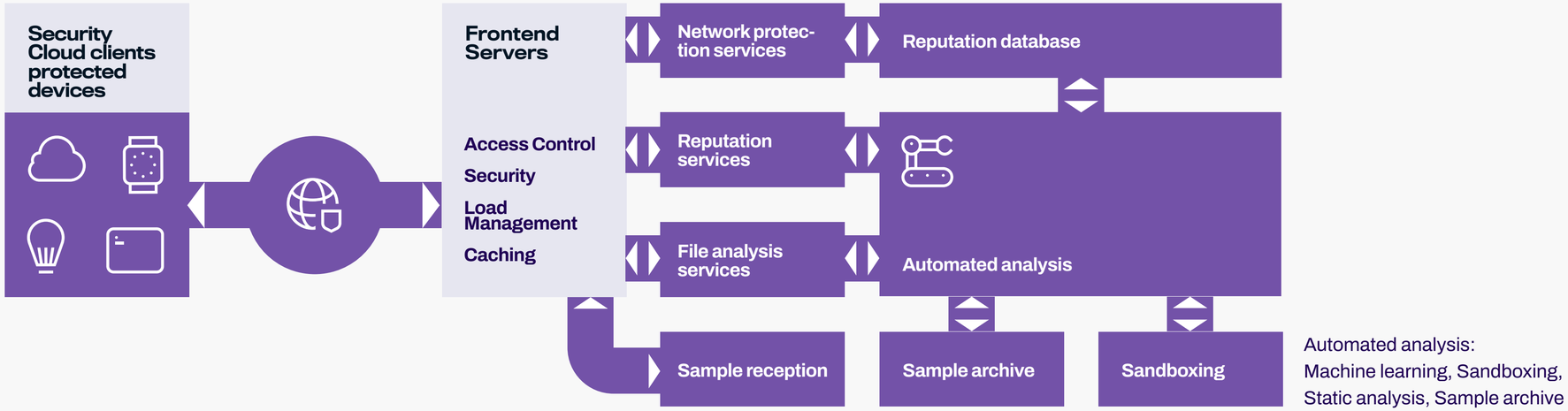
Faster detection speed

Products with local engines receive periodic updates to their definition databases. However, the frequency at which these updates arrive cannot be compared to the reaction speed of cloud-based systems. Because the Security Cloud relies on a cloud-based reputation database, new detections are instantly available for all clients using the Security Cloud services.

Added flexibility

The Security Cloud provides a range of independent services, and different products employ different sets of these services. This allows WithSecure™ to maintain a comprehensive portfolio of varying products on different operating systems that all benefit from cloud threat intelligence. Furthermore, the Security Cloud is continuously enhanced by technologies that include the latest malware analysis. The improved protection capabilities of the Security Cloud become available immediately to all Security Cloud-enabled products without the need of client upgrades or user actions.

How does the Security Cloud work?



Automated analysis:
Machine learning, Sandboxing, Static analysis, Sample archive

Overview

The Security Cloud is an online service that protects customer devices; that is, computers, mobile devices, routers, and other internet-connected devices that are present in people's homes and offices today. The picture below provides an overview of the Security Cloud's key functions.

The Security Cloud on the client side

The Security Cloud provides various services that individual security components on the client side can connect to. These client-side components are developed by WithSecure™. Products using the Security Cloud are mainly developed by WithSecure™, but some third parties may have an agreement with WithSecure™ to utilize one or more of these services in their own products and services.

Reputation services

One of the core components of the Security Cloud is WithSecure™ Karma™, the object reputation service, which assesses the safety of objects, thus avoiding a need for deeper analysis. Karma enables clients to query the reputation of computer networks, files, and web addresses. Files are checked by calculating their cryptographic hash and sending them to the reputation service. Web addresses are anonymized before sending them to the reputation service.

As site categorization is included for web addresses, the contents of the website can be identified. This allows for enhanced online banking security and parental controls, for example. The Security Cloud may request additional metadata or a sample of the previously unseen content for further analysis. Clients respond to such requests according to their user preferences and privacy policies.

Sample analysis services

Lightweight products rely mainly on WithSecure™ Mind™ for malware analysis. Mind, which is the Security Cloud's sample analysis service, works in conjunction with the reputation service Karma. If the reputation of a file is previously unknown, the client may be asked to upload the sample-related metadata to the Security Cloud for analysis. The results of the analysis may cause the sample to be flagged as suspicious and to be uploaded for further processing. Once the potentially heavy analysis, including the behavioral analysis, is done, every Security Cloud client subsequently benefits from the analysis and avoids waiting for the results.

Sample archive

WithSecure's sample archive contains files that the Security Cloud has received from a variety of sources. Both malicious and suspicious files may be present in this collection. Malicious files are generally archived permanently, whereas suspicious files are removed once they are not deemed malicious. A collection of highly common clean files is also maintained. Clean files from customer devices are not stored permanently.

Systems for malware analysis

Today's rapidly developing threat landscape requires a highly automated approach to malware analysis. Files and web addresses classified as suspicious are received from many sources and go through multi-layered analysis. This includes, but is not limited to, metadata analysis, structural analysis, statistical analysis, and behavioral monitoring. For example, software executables can be both statistically analyzed for malicious patterns, as well as executed in isolated sandboxes where their real behavior can be tracked for suspicious activity. The Security Cloud's algorithms examine sample metadata and analysis results, and either perform further analysis, or classify the object as either clean or malicious. Rare unclear cases can be flagged for manual inspection and may be examined by human experts for research purposes.

Some metrics from the Security Cloud*

The Security Cloud is a critical component that most devices protected by WithSecure™ technology use. This section presents figures depicting the volumes that the Security Cloud processes.

Approximate number of queries per day received by the Security Cloud services

2 billion

Approximate number of unique samples received per day by the Security Cloud

400 000

Files and web addresses blocked

Analysis results given in 100ms

*Year 2020

Security and privacy

Our services house a massive collection of malicious software that could be harmful if exposed. We therefore apply strict security practices when dealing with any data collected from client devices. All data is anonymized on the client before transmission to the Security Cloud. Data that could be used to determine the identity of the device or the user of a device is never collected. All network traffic between clients and the Security Cloud is always encrypted.

Privacy principles

Privacy is one of WithSecure's core values for all development and operations of the Security Cloud. We only ever collect the minimal amount of data required for providing the service. Our principle is that every transferred bit must be justifiable from a threat-fighting perspective, and that data is also never collected for presumed future needs. The following table documents our privacy principles in full detail.

Privacy principles	
We minimize the upstream of technical data	Data about customer devices is not collected and transferred unless the data is essential for providing the protection service.
We do not upstream personal data	The system is designed not to send any information that can identify a person using a device that communicates with the Security Cloud. Such data is not needed for the operation of the Security Cloud. Security Cloud-enabled clients use several algorithms to prevent private data from being transmitted and from filtering out such data from web addresses and file paths, for example.
We use anonymous identifiers	Clients generate unique anonymous identifiers that cannot be tied to the identity of the user, license owner, or device owner. These kinds of identifiers are used when repetitive connections from the same device need to be tracked.
We prevent the consolidation of backend data	Clients use several different unique anonymous identifiers for different connections to the Security Cloud. This makes it impossible for WithSecure™ to profile users by comparing user identifiers from different systems.
We never store IP addresses	Customers' IP addresses are never stored.
We do not trust the network	All network transfers are encrypted using strong encryption methods.

Security principles	
Secure by design	A system is never secure unless it has been designed to be secure, and we believe making a system secure as an afterthought is next to impossible. Having security as a core driver in the design process means we never have to sacrifice security for functionality.
Data encryption	Data is always encrypted at rest and in-transit using strong encryption methods.
Separated malware environments	Storing and analyzing malicious software is a challenging task in which we have over 30 years of experience. All malware handling is performed in networks separated from the internet and other WithSecure™ networks. Storage and analysis networks are isolated from each other, and files are transferred using strictly controlled methods.
Professional monitoring	All critical systems in the Security Cloud are monitored by WithSecure™ personnel. All systems storing or analyzing malware are operated by WithSecure™ and trusted partners.
Limited access	Only a limited number of WithSecure™ employees have access to the Security Cloud's critical systems. Such access is granted, revoked, and audited, according to a documented and controlled process.
An open attitude	The most fundamental principle in all security work is an open and humble attitude. We have put considerable effort into making the Security Cloud as secure as possible, and this work is a continuous process. A secure system can only be maintained by promoting an open attitude where problems in the system are reported, analyzed, and fixed promptly. This attitude includes transparency if we encounter incidents jeopardizing customer security. WithSecure™ encourages anyone who encounters security issues to get in touch, and we run a bug bounty program to reward such activity.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure